RNS representation for homomorphic encryption

Vincent Zucca*[1,2]

[1]Laboratoire dÍnformatique de Robotique et de Microélectronique de Montpellier – Université de Montpellier : UMR5506, Centre National de la Recherche Scientifique : UMR5506 – France
[2]Université de Perpignan Via Domitia – Laboratoire d'informatique, de robotique et de microélectronique de Montpellier (LIRMM) – France

Résumé

Lors de la dernière décénnie, le chiffrement (complètement) homomorphe a considérablement évolué en passant du stade d'idéal inatteignable à réalité. Le problème principal de ce genre de chiffrement étant la performance, un travail important a été réalisé au sein de la comunauté afin de rendre le chiffrement homomophe utilisable en pratique.
Parmi les différentes techinques utilisées pour améliorer leurs performances, certains chiffrements homomorphes font un usage intensif de la représentation des nombres par les résidus (RNS). Durant cet exposé, je présenterai la façon dont la représentation RNS est utilisée dans deux de ces schémas BGV et BFV. Bien qu'à priori théoritquement équivalent, les expériences menées par une partie de la communauté tendaient à montrer que BGV permettait d'effectuer plus d'opérations homomorphes que BFV.
Dans la suite de l'exposé, je démontrerait que ces deux schémas se comportent bien de manière similaire et que les différences précédemment observées résultaient en réalité d'une mauvaise initialisation de BFV. Je terminerai l'exposé en présentant une amélioration de l'implémentation RNS de BFV qui permet d'en améliorer un peu plus les performances afin de le rendre plus proche de BGV en pratique.

*Intervenant